Gauss's Theorem

statement :- The Product of two Primitive Polynomial over a UFD is a Primitive Polynomial.

Proof : Let R be a UFD and

let $f(x) = a_0 + a_1x + \cdots + a_nx^n$

$g(x) = b_0 + b_1x + \cdots + b_mx^m$

be two Primitive Polynomials over R.

$(a_0, a_1, \ldots a_n) = 1$

& $(b_0, b_1, \ldots b_m) = 1$

Let $f(x)\, g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n}$ — (1)

where $c_i = \sum_{r+s=i} a_r b_s \quad , 0 \le i \le m+n$

Let $(c_0, c_1, \ldots c_{m+n}) = d$

T.P d is a unit

If Possible suppose d is not a unit

$\exists$ an irreducible element p s.t. p / d

$\Rightarrow p / c_i$

We have $(a_0, a_1, \ldots a_n) =$ unit

$\Rightarrow p \nmid$ all a_i's

Let r be smallest suffix i.e. $p \nmid a_r$

Let s be smallest suffix i.e. $p \nmid b_s$

$\therefore p / a_0, p / a_1 \ldots p / a_{r-1}$

& $p / b_0, p / b_1 \ldots p / b_{s-1}$.

Scanned with ACE Scanner

By (1)

$$f(x)\,g(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{m+n} x^{m+n}$$

$$(a_0 + a_1 x + \dots + a_n x^n)(b_0 + b_1 x + \dots + b_m x^m) = c_0 + c_1 x + \dots + c_{m+n} x^{m+n}$$

Compare coeffs. of x^{r+s},

$$c_{r+s} = (a_0 b_{r+s} + a_1 b_{r+s-1} + \dots + a_{r-1} b_{s+1}) + a_r b_s + (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} \dots a_{r+s} b_0) \quad -(2)$$

Now $p \mid a_0,\ p \mid a_1 \dots p \mid a_{r-1}$

also $p \mid b_0,\ p \mid b_1 \dots p \mid b_{s-1}$

$\Rightarrow p \mid (a_0 b_{r+s} + a_1 b_{r+s-1} + \dots + a_{r-1} b_{s+1})$

& $p \mid (a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \dots + a_{r+s} b_0)$

Also $p \mid c_{r+s}$

$\Rightarrow p \mid c_{r+s} - (a_0 b_{r+s} + \dots + a_{r-1} b_{s+1}) - (a_{r+1} b_{s-1} + \dots + a_{r+s} b_0)$

$\Rightarrow p \mid a_r b_s$

$\Rightarrow p \mid a_r$ or $p \mid b_s$

Contradictions as $p \nmid a_r$ & $p \nmid b_s$

$\therefore d$ is a unit

Hence $f(x)\,g(x)$ is Primitive.

Scanned with ACE Scanner